CLAIMS

In the Claims:

1. A method for generating a random permutation of a countable sequence of unique numbers from zero to a maximum value N-1 comprising: and
   a. emitting a sequence of random numbers;
   b. discarding any duplicate values between 0 and N-1 of the sequence of random numbers;
   c. discarding any values greater than N-1 of the sequence of random numbers.

2. The method according to Claim 1 wherein emitting the sequence of random numbers is accomplished via a random number generator.

3. The method according to Claim 2 wherein the random number generator is a pseudo-random number generator.

4. A method for generating a random permutation of a countable sequence of unique numbers from zero to a maximum value N-1 comprising:
   a. generating a countable sequence of unique numbers numbers from zero to a maximum value N-1;
   b. generating a random number; and
   c. emitting a plurality of random bit vectors used to control a plurality of random shuffles.

5. The method according to Claim 4 wherein the random number is no less than 3/2 x $\log_2(N)$.

6. The method according to Claim 4 wherein generating the sequence of random numbers is accomplished by a random number generator.

7. The method according to Claim 4 wherein a number of the plurality of random bit vectors is at least equal to a value of the random number.

8. The method according to Claim 4 wherein a number of the plurality of random bit vectors is equal to the plurality of random shuffles.

9. The method according to Claim 6 wherein the random number generator is a pseudo-random number generator.

10. The method according to Claim 4 further comprising shuffling the sequence of numbers.

11. A method for generating a random permutation of a sequence of random numbers comprising:
   a. generating a sequence of random numbers;
   b. initializing a large random secret filled with the sequence of random numbers;
   c. initializing a random mixing seed with the random permutation of a sequence of unique random numbers;
   d. generating a random permutation of the sequence of random numbers based on the large random secret and the random mixing seed.

12. The method according to Claim 11 wherein the random mixing seed is a plurality of random mixing seeds.

13. A method for enciphering a sequence of clear text data values comprising:
   a. nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets;

09938790 .082401

b. performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads;

c. circularly rotating the values of each of the plurality of large random pads according to a plurality of random rotation values thus forming a plurality of rotated large random pads;

d. randomly shuffling a portion of each of the plurality of randomly rotated and large random pads according to a plurality of working keys thus forming a plurality of randomly rotated and randomly shuffled large random pads;

e. performing an exclusive OR function on the plurality of rotated and randomly shuffled large random pads to produce a final pad

f. selecting a portion of the final pad to form a finite key stream; and

g. performing an exclusive OR function with the finite key stream with the sequence of clear text data values.

14. The method according to Claim 13 further comprising substituting a value within each of the plurality of nested shuffled large random secrets with a new random value using a plurality of substitution keys thus forming a plurality of nested shuffled and substituted large random secrets.

15. The method according to Claim 13 further comprising substituting a value within each of the plurality of large random secrets with a new random value using a plurality of substitution keys thus forming a plurality of substituted large random secrets.

16. The method accordingt to Claim 13 further comprising selecting a series of portions of the final pad to form the finite key stream.

17. The method according to Claim 13 further comprising transmitting the plurality of random secrets, the plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a central server.

18. The method according to Claim 13 further comprising transmitting the plurality of random secrets, the plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a storage device.

19. A method for enciphering a sequence of cipher text data values comprising:

   a. nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets;
   b. performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads;
   c. circularly rotating the values of each of the plurality of large random pads according to a plurality of random rotation values thus forming a plurality of rotated large random pads;
   d. randomly shuffling a portion of each of the plurality of randomly rotated and large random pads according to a plurality of working keys thus forming a plurality of randomly rotated and randomly shuffled large random pads;
   e. performing an exclusive OR function on the plurality of rotated and randomly shuffled large random pads to produce a final pad
   f. selecting a portion of the final pad to form a finite key stream; and
   g. performing an exclusive OR function with the finite key stream with the sequence of cipher text data values.

20. The method according to Claim 19 further comprising substituting a value within each of the plurality of nested shuffled large random secrets with a new random value using a plurality of substitution keys thus forming a plurality of nested shuffled and substituted large random secrets.

21. The method accordingt to Claim 19 further comprising selecting a series of portions of the final pad to form the finite key stream.

22. The method according to Claim 19 further comprising transmitting the plurality of random secrets, the plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a central server.

23. The method according to Claim 19 further comprising transmitting the plurality of random secrets, the plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a storage device.

24. An apparatus for generating a keyed one-way hash value comprising:

a. a rotation pool for providing a plurality of rotation vectors, each of the plurality of rotation vectors consisting of a series of random rotation values;

b. a plurality of lookup tables containing random values in a table entry;

c. a compression function configured to receive a block of message data, a rotation vector containing the series of random rotation values, a plurality of padding values, and outputs a final compression value; and

d. a mechanism connected to the plurality of look-up tables configured to substitute a random hash value for the final compression value.

25. The apparatus according to Claim 24 further comprising an encryption pool for providing encryption pads.

26. The apparatus according to Claim 25 further comprising a one time pad encipherment of the hash value using a pad extracted in a unique manner from the encryption pool, resulting in a message authentication code value.

27. The apparatus according to Claim 24 further comprising a padding pool for providing random padding values.

28. The apparatus according to Claim 27 further comprising a plurality of random padding values.

29. The apparatus according to Claim 24 further comprising a tree construction of multiple, cascaded compression functions, which input multiple message blocks and outputs the final compression value.